

Chapter 23: Installing and Configuring MIT

Kerberos on a Macintosh System

In this chapter we describe how to install and configure the **MIT Kerberos for Macintosh 4.0x** software¹ on your Macintosh system in order to access Kerberized machines and encrypt your data transmissions.

Computing Division Macintosh Strategy

The Computing Division released a statement in January 2001 regarding the policy on Macintosh support. We quote from it here:

“The Macintosh Operating System is no longer a supported operating system from the Computing Division and is not a strategic operating system for future plans...

... Specifically regarding the Strong Authentication realm, the supported access method from Macintoshes will be via the CRYPTOCARD. Kerberos clients may be available and used, but there will be no effort expended to select, test or distribute them.”

That said, there is some community support for the Macintosh, primarily through *kerberos-users@fnal.gov*. We also provide information here to assist Macintosh users.



We do not currently have a recommendation for Macintosh users outside of the U.S. and Canada. MIT does not yet interpret U.S. regulations as allowing export, so it is the responsibility of the downloader to be in compliance. MIT's statement on Kerberos export control is maintained at

<http://web.mit.edu/kerberos/www/export.html>. The MIT Kerberos software for Macintosh is not made freely available on the <http://www.crypto-publish.org/> web site because it includes code built from non-open sources. You may want to consider upgrading your OS to OS X and using the Kerberos software for UNIX.

1. Version 4.0a12 has since been made available.

23.1 Installing MIT Kerberos for Macintosh

First, obtain a Kerberos principal and initial password for the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal*.

This section was originally written for version 3.5 of the MIT kerberos software for Macintosh. Various versions 4.0x have since been made available. Installation can be accomplished by clicking on the “Kerberos for Mac 4.0” installer application. This should install everything into the disk containing your System Folder. This version includes the Kerberos Floating Window (for status), and Kerberos Menu on the menubar (a quick way to create/destroy tickets and to open the Kerberos Control Panel). You will need to reboot probably twice, then, assuming your Kerberos Preferences file is configured properly, you should successfully get a ticket for your principal.

Note that MIT Kerberos for Macintosh was shipped as part of Mac OS X in the OS X 10.1 update shipped by Apple. There is a kit of “extras” for OS X 10.1 with some additions to what was shipped with the OS. See <http://web.mit.edu/macdev/Development/MITKerberos/Common/Documentation/osx-kerberos-extras.html>.

23.1.1 Changes in MIT Kerberos for Macintosh 4.0

See

<http://web.mit.edu/macdev/Development/MITKerberos/Common/Documentation/release-4.0.html>. A big change is better OS X support. User interface changes relative to v3.5 include:

- The **KERBEROS CONTROL PANEL** is a changed version of the **KERBEROS MANAGER**.
- The **KERBEROS MENU** on the menu bar shows the status of the active user’s TGT and can be used to quickly get/destroy/renew tickets or open the control panel.
- The **KERBEROS CONTROL STRIP** is similar to the **KERBEROS MENU** but a module in the control strip.
- Kerberos Floating Window
- Optional status display of all user’s TGTs.

Regarding installation, version 4.0 includes two installer programs, one for OS X and the other for OS 8/9 (supports 8.1 through 9.2.1) but is otherwise much the same as version 3.5.

23.1.2 Download Kerberos from the MIT Web Site

- 1) Bring up the **MIT Kerberos for Macintosh** web page, at URL `http://web.mit.edu/macdev/www/kerberos.html`.
- 2) Select *Getting MIT Kerberos for Macintosh*.
- 3) On this page, look for the paragraph that starts “If you are outside of MIT but still in the US or Canada...”. Click on the *download page* link in that paragraph.
- 4) This brings you to the **Kerberos Distribution Authorization Form**. Answer the three questions, and submit the form to arrive at the download page. (There is a link on this page for Canadian users, which we have not tried or documented.)
- 5) Click on the link for MIT Kerberos for Macintosh 4.
- 6) Under the small heading “Binaries and SDKs”, click *Binhexed self mounting disk image*.

23.1.3 Items that Appear on your Desktop

You’ll find three new items on your desktop once the transfer finishes (This section has not been updated since v3.5; you will find similar things for v4.0.):

- MIT Kerberos for the Mac folder
- MIT_Kerberos_for_Mac_3.5.hqx file
- MIT Kerberos for Mac 3.5.smi file

There will also be a new disk volume from mounting the .smi (if the disk is not present, double-click the .smi file).

Discard the .hqx file, and open the MIT Kerberos for the Mac folder. This folder contains:

- two subfolders:
 - Mac OS 9 Binaries 3.5, which contains four sub-subfolders labelled as per their destination folders (the names are of the form ->Into <Foldername>)
 - Mac OS 9 SDK 3.5; this is the software development kit and can be ignored.
- one application program **Kerberos for Mac 3.5**
- three links/HTML files: to the MIT Kerberos home page, to the Kerberos for Macintosh Bugs page, and to the KfM 3.5 Release Notes.
- one text file KfM 3.5 Read Me, which contains installation instructions



The Kerberos for Macintosh 4.0 disk will have similar contents with the addition of the "Kerberos for Mac OS X 4.0" application and a link "Mac OS X SDK Information". Note that 4.0 supports both Mac OS 8.1 through 9.1 as well as Mac OS X.

23.1.4 Installation Instructions

(This section has not been updated since v3.5; v4.0 is similar.) We refer you to the Read Me file to complete the installation of MIT Kerberos for the Mac, but we provide a few clarifications here:

- On the MIT download page, double-click the Kerberos for Mac 3.5 application to install.
- The downloaded files no longer need to be copied manually into folders under the System Folder on your system.
- The ->Into Preferences folder contains three subfolders. Choose Kerberos Preferences v5.

After installation, if you get the error message "preauthentication fails" when you attempt login via the **GET TICKETS** button, it is most likely caused by a password or time-sync error. First verify your password is correct. Then, synchronize your machine with the network time (follow the instructions at <http://hdstock.mit.edu/answers/102.html>). The Date & Time control panel under OS 8.6 and later allows one to select a Network Time Server. The Apple time server (time.apple.com) can be used.

23.2 Configuring the Kerberos Software

23.2.1 The Preferences File

The Kerberos Preferences file needs to contain information for Fermilab's strengthened realm(s). Edit the file or just replace the initial contents with that of the `krb5.conf` file from either the **krb5conf** product in KITS or a machine in the Fermilab FNAL.GOV realm (note that pasting text directly from a web browser may cause end-of-line problems). A Fermi-configured Preferences file is now available for download from <http://www.fnal.gov/docs/strongauth/ps/> (see `Kerberos_Preferences.sit` for the StuffIt archive file, or `Kerberos_Preferences.hqx` for the BinHexed (ASCII encoding) version of that file). We reproduce the text of the file here:

```
[libdefaults]
    default_realm = FNAL.GOV
```

```

ticket_lifetime =1560
checksum_type = 1
ccache_type = 2
default_tkt_enctypes = des-cbc-crc
default_tgs_enctypes = des-cbc-crc
noaddresses = true

[realms]
    FNAL.GOV = {
        kdc = krb-fnal-1.fnal.gov:88
        kdc = krb-fnal-2.fnal.gov:88
        kdc = krb-fnal-3.fnal.gov:88
        kdc = krb-fnal-4.fnal.gov:88
        kdc = krb-fnal-5.fnal.gov:88
        admin_server = krb-fnal-admin.fnal.gov
        default_domain = fnal.gov
        auth_to_local =
RULE:[1:$1@$0](.*@PILOT\.FNAL\.GOV)s/@.*//
        auth_to_local = DEFAULT
    }
    PILOT.FNAL.GOV = {
        kdc = krb-pilot-1.fnal.gov:88
        kdc = krb-pilot-3.fnal.gov:88
        kdc = krb-pilot-4.fnal.gov:88
        kdc = krb-pilot-5.fnal.gov:88
        admin_server = krb-pilot-admin.fnal.gov
        default_domain = fnal.gov
        auth_to_local =
RULE:[1:$1@$0](.*@FNAL\.GOV)s/@.*//
        auth_to_local = DEFAULT
    }
    WIN.FNAL.GOV = {
        kdc = newpckits.fnal.gov:88
        admin_server = newpckits.fnal.gov
        default_domain = fnal.gov
    }

[domain_realm]
    .fnal.gov = FNAL.GOV
    .hep.net = FNAL.GOV
    .minos-soudan.org = FNAL.GOV

```

Note: if you have to deal with Network Address Translation (NAT), see section 5.9.4 *Network Address Translation*.

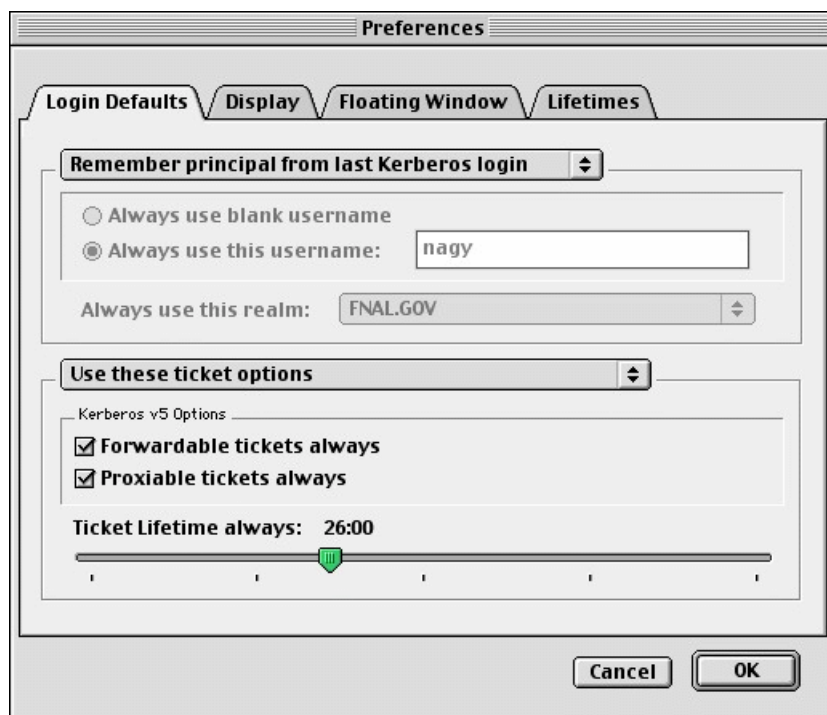
23.2.2 Select Favorite Realms

After modifying the **KERBEROS PREFERENCES**, start the **KERBEROS CONTROL PANEL** and select the **FAVORITE REALMS** item from the **EDIT** menu. Use the dialog box to copy your favorite realms from the right to the left-hand side of the screen.

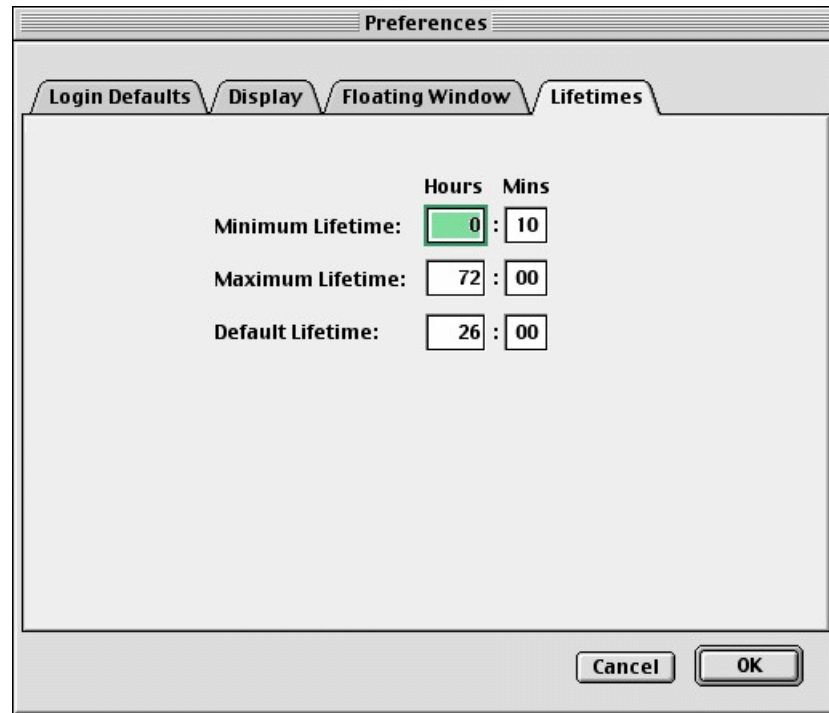


23.2.3 Edit Preferences

Edit your login preferences, and make sure you check **FORWARDABLE TICKETS ALWAYS**:



Edit your ticket lifetime preferences (the KDC limits the ticket lifetime to 26 hours):



23.2.4 Edit Favorites

23.3 Installing Telnet Client

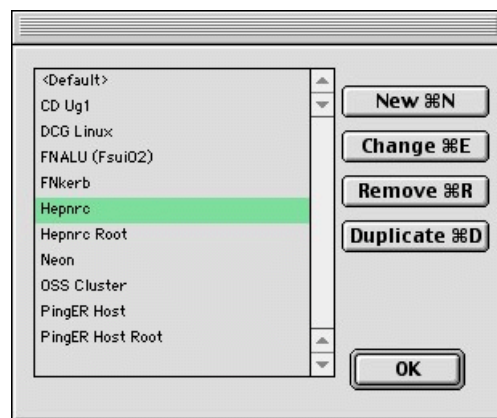
BetterTelnet and **NiftyTelnet** with Kerberos v5 support are the only **telnet** products that we know of at this time that work on the Macintosh. We document **BetterTelnet** here. You'll need both it and an associated plug-in installed on your machine.

- 1) Bring up the **MIT Kerberos for Macintosh** web page, at URL `http://web.mit.edu/macdev/www/kerberos.html`. Select *Frequently Asked Questions*.
- 2) Look for the Q/A that discusses **telnet** (you can search on "BetterTelnet"). Click on the link *BetterTelnet and Kerberos plugin*. This brings you to the FTP site:
`ftp://ftp.cmf.nrl.navy.mil/pub/chas/MIT_Kerberos_3.5/`.
- 3) If you don't already have **BetterTelnet** installed, click on `BetterTelnet 2.0f...` and install this software first.

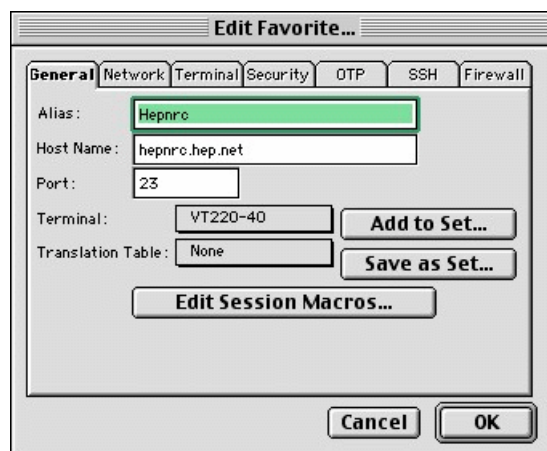
- 4) Once **BetterTelnet** is installed, download `Telnet_Plugin.bin` from the same **FTP** site and copy it to the **BetterTelnet** folder on your machine.

23.4 Configuring Telnet

- 1) Invoke **BetterTelnet**. On the **FAVORITES** menu, choose **EDIT FAVORITES**. You should create one configuration for each strengthened host you plan to access.

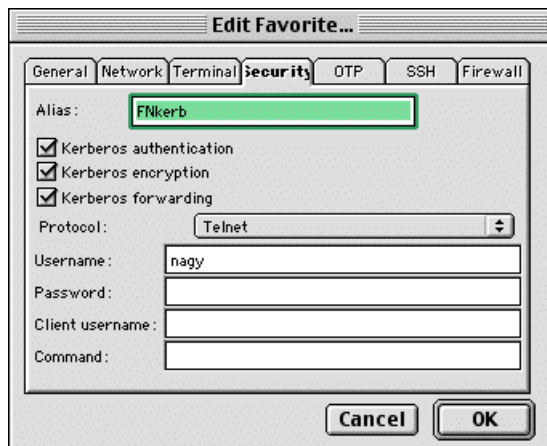


- 2) To create a new configuration, on the pop-up screen, click **NEW**. Then, with the **GENERAL** tab selected, type in an **ALIAS** which will be used to identify the host (this can be any string) and the **HOST NAME**.



- 3) **Very important!!** Change to the **SECURITY** tab, check Kerberos authentication and Kerberos encryption. Kerberos

forwarding is recommended. The protocol should be left as telnet (the default). Filling in other fields is optional (even if you fill in your Kerberos password, you need to provide it again when you authenticate). Click **OK** to save the configuration.



23.5 Kerberized FTP Client

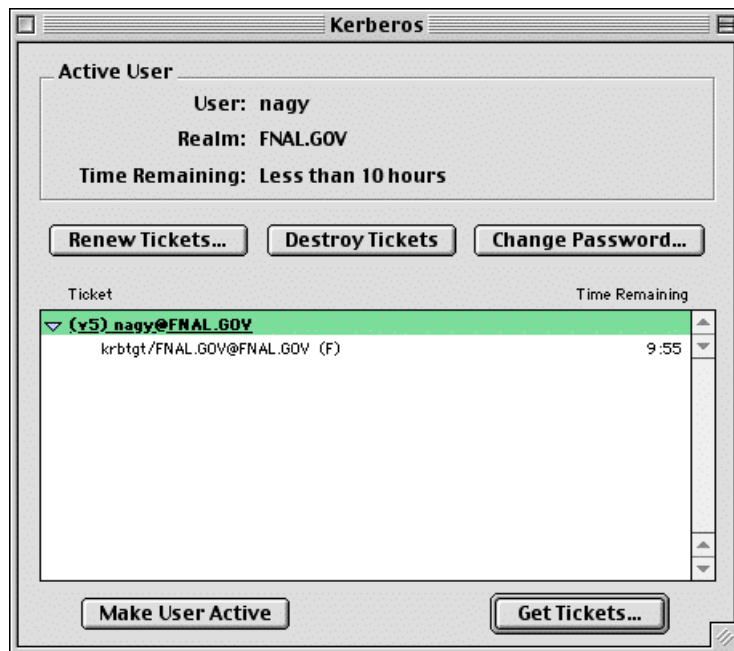
Fetch 3.0.4 beta Secure is freeware for Macintosh. It can be downloaded from the MIT Kerberos Distribution Page at <http://web.mit.edu/network/kerberos-form.html>.

Also, Fetch 4.0 is shareware available from Fetch Softworks at <http://www.fetchsoftworks.com/>. Installation instructions are not provided here (at least not yet!).

23.6 Authenticating to Kerberos

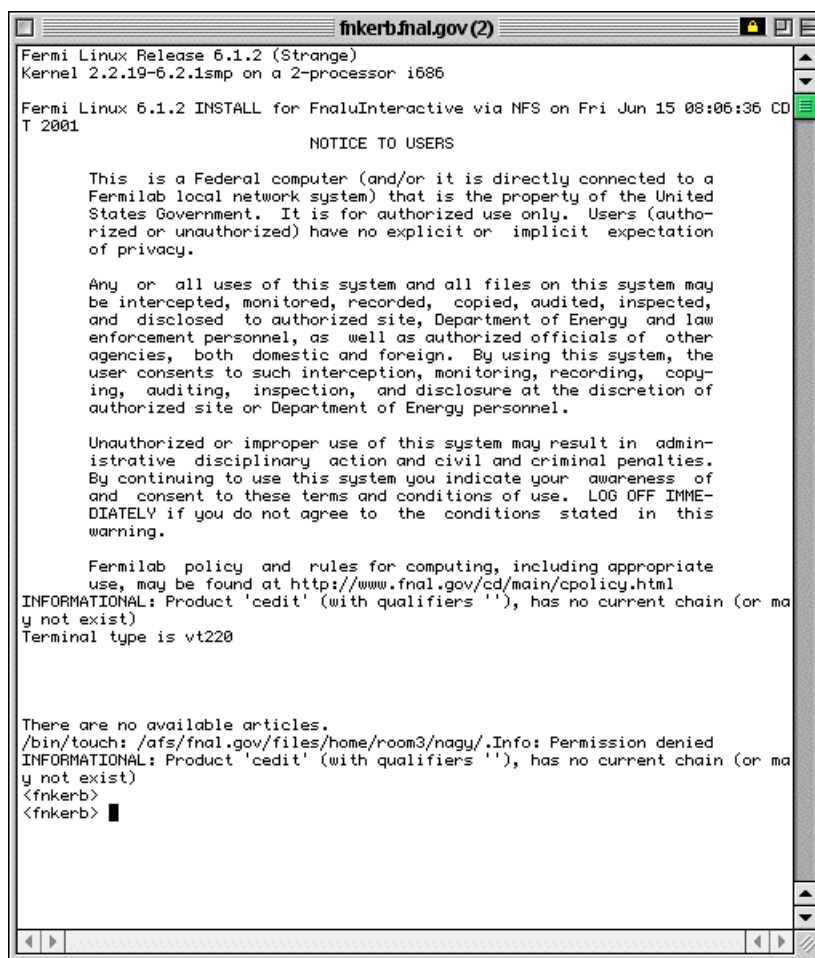
23.6.1 Authenticate via Kerberos Control Panel

- Invoke the **Kerberos Control Panel** (from **CONTROL PANELS** under the Apple menu, from the **KERBEROS MENU** in the menu bar, or from the **KERBEROS CONTROL STRIP** module).



- Select principal, and click **GET TICKETS**.
- Enter your Kerberos password on the pop-up screen.

You should see a ticket appear. Now you can invoke your **telnet** product (**BetterTelnet** or **NiftyTelnet**) and connect to one or more strengthened hosts without having to provide your password again.



```
fnkerbfnal.gov (2)
Fermi Linux Release 6.1.2 (Strange)
Kernel 2.2.19-6.2.1smp on a 2-processor i686

Fermi Linux 6.1.2 INSTALL for FnalInteractive via NFS on Fri Jun 15 08:06:36 CD
T 2001

NOTICE TO USERS

This is a Federal computer (and/or it is directly connected to a
Fermilab local network system) that is the property of the United
States Government. It is for authorized use only. Users (author-
ized or unauthorized) have no explicit or implicit expectation
of privacy.

Any or all uses of this system and all files on this system may
be intercepted, monitored, recorded, copied, audited, inspected,
and disclosed to authorized site, Department of Energy and law
enforcement personnel, as well as authorized officials of other
agencies, both domestic and foreign. By using this system, the
user consents to such interception, monitoring, recording, copy-
ing, auditing, inspection, and disclosure at the discretion of
authorized site or Department of Energy personnel.

Unauthorized or improper use of this system may result in admin-
istrative disciplinary action and civil and criminal penalties.
By continuing to use this system you indicate your awareness of
and consent to these terms and conditions of use. LOG OFF IMME-
DIATELY if you do not agree to the conditions stated in this
warning.

Fermilab policy and rules for computing, including appropriate
use, may be found at http://www.fnal.gov/cd/main/cpolicy.html
INFORMATIONAL: Product 'cedit' (with qualifiers ''), has no current chain (or ma
y not exist)
Terminal type is vt220

There are no available articles.
/bin/touch: /afs/fnal.gov/files/home/room3/nagy/.Info: Permission denied
INFORMATIONAL: Product 'cedit' (with qualifiers ''), has no current chain (or ma
y not exist)
<fnkerb>
<fnkerb> █
```

23.6.2 Authenticate at Login

Invoke **BetterTelnet** or **NiftyTelnet** and connect to a strengthened host. You will be prompted for your Kerberos password, and then authenticated once you have provided it.

